UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF MISSOURI

LEAH WILLIS, on behalf of all others similarly situated, Plaintiff, v. ASCENSION HEALTH, Defendant.	**CASE NO.:** **CLASS ACTION COMPLAINT** **JURY TRIAL DEMANDED**

Plaintiff Leah Willis ("Plaintiff"), by and through her attorneys, individually and on behalf of all others similarly situated, brings this Class Action Complaint ("Complaint") against Defendant Ascension Health ("Ascension Health" or "Defendant") and makes the following allegations based upon knowledge as to herself and her own acts, and upon information and belief as to all other matters, as follows:

INTRODUCTION

1. Ascension Health is one of the nation's leading and most trusted health systems, which includes 140 hospitals and generates approximately $28 billion dollars in annual revenue.[1]

2. As part of its business in providing health care, Defendant collects from its patients, among other things, patients' names, contact information, Social Security numbers, insurance information, payment information, exam and/or procedure information, referring physicians, as well as diagnosis information and medical histories.

[1] https://about.ascension.org/news/media-resources (last visited June 7, 2024).

3. In its Privacy Policy, Defendant claims that they are "committed to maintaining the privacy and confidentiality of your health information." In their Joint Notice of Privacy Practices for Michigan patients, Defendant touts that it will: 1) maintain the privacy and security of protected health information under requirement of law; 2) notify patients promptly if a breach occurs that may have compromised the privacy or security of protected information; 3) follow the duties and privacy practices described in the notice; and 4) not use or share information other than as described in the notice without a patient's written consent.[2]

4. However, according to Defendant's initial Notice posted on their website, Defendant became aware of "unusual activity" on its network systems on May 8, 2024 and determined that an unauthorized party had access to its network and documents in that system.[3] For an undisclosed amount of time, the unauthorized third party gained access to the personally identifiable information ("PII") and protected health information (PHI") of the patients, potentially including the names, dates of birth, patient records, Social Security numbers, and other information (collectively, "Private Information") maintained by Defendant (the "Data Breach").[4]

5. According to the Federal Trade Commission ("FTC"), PII is "information that can be used to distinguish or trace an individual's identity, either alone or when combined with other information that is linked or linkable to a specific individual."[5] PHI is deemed private under the Healthcare Insurance Portability and Accountability Act of 1996 ("HIPAA"), 42 U.S.C. §§ 1320d, *et seq.*, as well as multiple state statutes.

---

[2] *See* https://healthcare.ascension.org/npp (last visited June 7, 2024).
[3] *See* https://about.ascension.org/cybersecurity-event (last visited June 7, 2024).
[4] *See id*.
[5] *See Federal Trade Commission Privacy Impact Assessment: Redress Enforcement Database (RED)* at 3, n.3, FTC (June 2019), https://www.ftc.gov/system/files/attachments/privacy-impact-assessments/redress_enforcement_database_red_privacy_impact_assessment_june_2019.pdf. (last visited June 7, 2024)

6. Defendant's failure to adequately protect its network has led to a nationwide shutdown of its network, which had not been restored as of the beginning of June, 2024 and is not expected to be fully restored until June 14, 2024.[6] Defendant has not only left its patients with distress for their exposed personal information, but left its network of providers no other choice but to perform their duties with a mere pen and paper system.[7] Defendant's failure has also impeded its ability to provide timely, vital healthcare to its patients.

7. Defendant's failure to ensure that its services and information were adequately secure fell far short of its legal obligations and Plaintiff's and Class Members' reasonable expectations for data privacy, jeopardized the security of their Private Information, violated applicable data privacy laws, and has put Plaintiff and Class Members at serious risk of fraud and identity theft.

8. Additionally, Plaintiff and Class Members were injured by the Data Breach because their medical procedures had to be cancelled, rescheduled or have been postponed.

9. Defendant failed to disclose that its data systems were not secure and, thus, vulnerable to attack. Had this been disclosed, Defendant would have been unable to continue obtaining business from patients and would have been forced to adopt and invest in reasonable data security measures and comply with the law. Defendant promised to protect the Private Information of patients but chose to ignore this promise by skimping on the security of its data systems.

10. Plaintiff brings this class action alleging that Defendant's conduct, as described

---

[6] *See* https://www.healthcarefinancenews.com/news/ascension-expects-ehr-restoration-across-its-network-june-14 (last visited June 7, 2024); https://www.detroitnews.com/story/news/local/michigan/2024/06/05/ascension-to-restore-michigan-electronic-health-record-systems-by-june-14/73989009007/ (last visited June 7, 2024).

[7] *See* https://www.nytimes.com/2024/05/23/health/cyberattack-ascension-hospitals-patient-data.html (last visited June 7, 2024).

more fully herein, caused Plaintiff's and Class Members' Private Information to be exposed and stolen and impaired Plaintiff's and Class Members' ability to obtain necessary healthcare from Defendant, because of the failure of Defendant to safeguard and protect their sensitive information. Plaintiff seeks damages, and injunctive and other relief, on behalf of herself and similarly situated consumers.

PARTIES

11. Plaintiff Leah Willis is a resident of Wayne County, Michigan and a patient of Ascension Providence Hospital – Southfield Campus, Southfield, Michigan. Plaintiff disclosed her Private Information to Defendant in accordance with its conditions to provide healthcare services.

12. Defendant Ascension Health is a Missouri corporation with its principal place of business in St. Louis, Missouri and headquarters located at 4600 Edmundson Rd., St. Louis, Missouri 63134.

JURISDICTION

13. This Court has jurisdiction over the subject matter of this action pursuant to 28 U.S.C. § 1332, as amended by the Class Action Fairness Act of 2005, because the matter in controversy exceeds $5,000,000, exclusive of interest and costs, and is a class action in which some members of the Class are citizens of different states than Defendant. *See* 28 U.S.C. § 1332(d)(2)(A). This Court has supplemental jurisdiction over the state law claims pursuant to 28 U.S.C. § 1367.

14. This Court has personal jurisdiction over Ascension Health because it is authorized to and conducts business in Missouri, has specifically marketed, advertised, and made substantial revenue in Missouri, and has sufficient minimum contacts with this state and/or sufficiently avails itself of the markets of this state through its promotion, revenue, and marketing within this state to

render the exercise of jurisdiction by this Court permissible.

15. Venue in this Court is proper pursuant to 28 U.S.C. § 1391 because Defendant does substantial business in this District, has intentionally availed itself of the laws and markets within this District through its promotion, marketing, and business activities in this District, and a significant portion of the facts and circumstances giving rise to Plaintiff's Complaint occurred in or emanated from this District.

FACTUAL ALLEGATIONS

A. Background

16. Defendant is "one of the nation's leading non-profit and Catholic health systems" with a network that includes over 140 hospitals in 19 states and the District of Columbia.[8]

17. For Plaintiff and Class Members to receive care from Defendant's health system, Defendant required that Plaintiff and Class Members' disclose sensitive, protected personal and health information to be stored in Defendant's data network.

18. Defendant used Plaintiff's and Class Members' personal and health information to conduct regular business throughout its national network.

19. In Defendant's Notice of Privacy Practices on their website, they maintain that Defendant is "committed to maintaining the privacy and confidentiality" of their patients' information, and that they are "required by law to maintain the privacy and security of [their patients'] identifiable health information."[9]

20. Plaintiff and Class Members take reasonable steps to protect their sensitive personal and health information. In trusting their healthcare to Defendant, they believed that Defendant

[8] https://about.ascension.org/about-us (last visited June 7, 2024).
[9] chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://healthcare.ascension.org/-/media/healthcare/npp/michigan/mi_ascension-michigan_english.pdf (last visited June 7, 2024).

would take reasonable steps within industry standards to secure and safeguard their information and that Ascension would be able to access such information in order to provide healthcare to them.

B. The Data Breach

21. On May 9, 2024, Defendant posted a notice titled "Cybersecurity Event Update" (The Notice) on their website stating that:

> On May 8, Ascension detected unusual activity in our network systems. We have determined this is a cybersecurity incident. We are working around the clock with internal and external advisors to investigate, contain, and restore our systems following a thorough validation and screening process. Our investigation and restoration work will take time to complete, and we do not have a timeline for completion.
>
> Systems that are currently unavailable include our electronic health records system, MyChart (which enables patients to view their medical records and communicate with their providers), some phone systems, and various systems utilized to order certain tests, procedures and medications. We have implemented established protocols and procedures to address these particular system disruptions in order to continue to provide safe care to patients. Out of an abundance of caution, however, some non-emergent elective procedures, tests and appointments have been temporarily paused while we work to bring systems back online. Our teams are working directly with any patient whose appointment or procedure will need to be rescheduled. We understand the frustration this may cause and sincerely regret any inconvenience to our patients.
>
> Due to downtime procedures, several hospitals are currently on diversion for emergency medical services in order to ensure emergency cases are triaged immediately. If you are experiencing a medical emergency, please contact 911 and your local emergency services will bring you to the nearest hospital emergency room.[10]

22. The Notice failed to include critical information, such as: (i) the actual date(s) of the Data Breach, (ii) what vulnerabilities in Defendant's system caused the Data Breach, (iii) the identity of the group that committed the Data Breach, and (iv) the measures Defendant was taking to prevent additional attacks since the Data Breach.

23. News reports later established that Defendant was targeted by a ransomware attack

[10] https://about.ascension.org/en/cybersecurity-event (last visited June 7, 2024).

by the group, Black Basta, which according to the New York Times "may be linked to Russian-speaking cybercriminals."[11]

24. When hospitals and healthcare systems are subject to ransomware attacks, they have "little choice" but to completely shut down their computer systems, forcing Defendant's providers and staff to resort to pen and paper operations to care for millions of patients.[12]

25. The Data Breach has since caused Defendant to completely "shut down" their network system for more than three weeks as of the beginning of June, 2024, forcing their providers and healthcare workers to attempt regular business with "no access to medical records, no access to labs, no access to radiology or x-rays, no ability to place [medical] orders."[13] While Ascension Health has restored its records systems in a few of the States in which it operates, it remains shutdown in Michigan and many other States and is not expected to be restored until June 14, 2024, more than a month after Ascension Health noticed the Data Breach.

26. Providers have expressed concern that "certainly patient care will be negatively impacted" due to the Data Breach. They have also stated that the failure to maintain protected data systems increases their "risk of an adverse event…."[14]

27. Defendant's network shutdown has caused many delays in patient care nationwide, including delays in receiving test results and diagnoses.[15] Patients even report delays in results needed to determine care to prevent harm to "vital organs."[16]

---

[11] https://www.nytimes.com/2024/05/23/health/cyberattack-ascension-hospitals-patient-data.html (last visited June 7, 2024).
[12] *Id*.
[13]https://www.freep.com/story/news/health/2024/05/09/ascension-hospital-cyberattack-data-breach-hacked-michigan/73620340007/ (last visited June 7, 2024).
[14] *Id*.
[15] *See* https://www.wbay.com/2024/05/31/ascension-patient-forced-spend-time-money-receive-care-after-cyberattack/ (last visited June 7, 2024).
[16] *Id*.

28. One Michigan patient reported having to wait seven (7) hours to receive pain medication after seeking care at Ascension Providence Hospital, and eventually discharged himself because he could not take the pain and was worried for his health.[17]

29. The Data Breach has also caused surgeries and procedures to be delayed and rescheduled, including sensitive procedures such as cancer screenings and ultrasounds.[18]

30. Patients claim these delays caused by the shutdowns have impacted them "[p]hysically," "[e]motionally," and now "financial[ly]."[19]

31. Plaintiff and Class Members believe that their personal information was or soon will be released on the dark web to be sold or exchanged for fraud and identity theft schemes. In addition, as a result of the Data Breach, Plaintiff and other Class Members have been deprived of important healthcare treatment, including surgery and other needed medical care.

32. In a Notice posted on Defendant's website on May 21, Ascension addressed the lack of system access by stating "[p]atients should continue to monitor [their website] for the latest information on a state-by-state basis."[20] The most recent "Cybersecurity Event Update" on Ascension's website, dated June 5, 2024, states that Ascension Health has "successfully restored EHR access in our Florida, Alabama, Tennessee, Maryland, and Central Texas (Ascension Seton and Dell Children's hospitals) markets" and that "we are working toward completing EHR restoration across our entire ministry by the end of the week ending June 14."[21] However, mere restoration of its systems will not undo either (1) the continued exposure of patients' Personal

[17] *See* https://www.fox2detroit.com/news/patients-leave-ascension-amid-cyber-attack-systems-remain-down (last visited June 7, 2024).
[18] *See* https://www.wrtv.com/news/local-news/ascension-patients-cyber-attack-causing-delays-for-medical-results (last visited June 7, 2024).
[19] *See* https://www.wbay.com/2024/05/31/ascension-patient-forced-spend-time-money-receive-care-after-cyberattack/ (last visited June 7, 2024).
[20] *See* https://about.ascension.org/en/cybersecurity-event (last visited June 7, 2024).
[21] *Id.*

Information to cybercriminals; and (2) the lack of access to timely medical care and treatment during the shutdown.

C. Ascension Healthcare Failed to Comply with Industry and Regulatory Standards

33. Defendant's failure to take reasonable, industry-standard security practices caused Plaintiff and Class Members' private, valuable information to be stolen by dangerous cybercriminals whose *modus operandi* is often to sell stolen data on the dark web and/or hold it for ransom for the victims to purchase back while causing significant business disruptions.

34. Because of the value of Private Information to cybercriminals and identity thieves, companies in the business of storing, maintaining, and securing Private Information, such as Ascension Health, have been identified as being particularly vulnerable to cyber-attacks. Cybersecurity firms have promulgated a series of best practices that, at minimum, should be implemented by sector participants including, but not limited to: encrypting patient information; deleting patient information when no longer needed; installing appropriate malware detection software; monitoring and limiting the network ports; protecting web browsers and email management systems; setting up network systems such as firewalls, switches and routers; monitoring and protection of physical security systems; protection against any possible communication system; and training staff regarding critical points.[22]

35. Defendant was also on increased notice, due to the many high-profile cybersecurity attacks on medical insurers and healthcare conglomerates, including recent incidents involving Change and United Healthcare that have targeted large national healthcare networks.[23]

---

[22] *See White Paper: Addressing BPO Information Security: A Three-Front Approach*, DATAMARK, Inc. (Nov. 2016), https://insights.datamark.net/addressing-bpo-information-security/. (last visited June 7, 2024).

[23] https://www.nytimes.com/2024/03/29/health/cyber-attack-unitedhealth-hospital-patients.html (last visited June 7, 2024).

36. Healthcare companies have become notorious targets for cybercriminals, and consistently named one of the "most susceptible" industries to cyber attacks because of the increased level of data collection by healthcare entities and the industry's failure to update their systems with technology that is compatible with the latest cybersecurity standards.[24]

37. Healthcare records can also be sold for exponentially larger amounts than financial information because they cannot be modified, and it is much easier for cybercriminals to commit healthcare fraud. Health diagnoses cannot be "canceled" and replaced, according to the national advisor for cybersecurity.[25]

38. Further, health records contain sensitive information that could lead to patient distress if made public. When one healthcare network refused to pay the ransom during a recent attack, the hackers posted explicit photographs of patients receiving breast cancer treatment.[26]

39. Defendant knew or should have known that they were at an exponentially increased risk to be targets of a ransomware attack for the reasons outlined above, and therefore should have implemented the proper safety procedures to protect Plaintiff and other patients' sensitive, highly valuable information, and to ensure that its provision of healthcare service to patients was not interrupted.

40. Had Defendant taken even minimal measures, such as encrypting patient information, Plaintiff and Class Members would not be at risk of their personal and health information being sold on the dark web and imminent fraud, or being deprived of healthcare services.

[24] *Id.*
[25] *Id.*
[26] *Id.*

41. Federal and state governments have likewise established security standards and issued recommendations to diminish data breaches and the resulting harm to consumers and financial institutions.

42. Defendant was prohibited by the Federal Trade Commission Act ("FTC Act") (15 U.S.C. § 45) from engaging in unfair or deceptive acts or practices in or affecting commerce. The Federal Trade Commission ("FTC") has concluded that a company's failure to maintain reasonable and appropriate data security for consumers' sensitive personal information is an "unfair practice" in violation of the FTC Act. *See, e.g., FTC v. Wyndham Worldwide Corp*., 799 F.3d 236 (3d Cir. 2015).

43. The FTC has promulgated numerous guides for businesses that highlight the importance of implementing reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision-making.

44. In 2016, the FTC updated its publication, Protecting Personal Information: A Guide for Business, which established cybersecurity guidelines for businesses. The guidelines note that businesses should protect the personal customer information that they keep; properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand their network's vulnerabilities; and implement policies to correct any security problems.

45. The FTC further recommends that companies not maintain PII longer than is needed for authorization of a transaction; limit access to private data; require complex passwords to be used on networks; use industry-tested methods for security; monitor for suspicious activity on the network; and verify that third-party service providers have implemented reasonable security measures.

46. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect customer data, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

47. Defendant also had a duty to safeguard Plaintiff's and Class Members' PHI under HIPAA and its implementing regulations, 45 C.F.R. §§ 160, *et seq*., which establish privacy and security standards for certain health organizations. Defendant is a "health care provider" subject to HIPAA because it receives, maintains, or transmits its patients' PHI.[27] "PHI" includes, in relevant part, individually identifiable health information relating to the provision of health care.

48. For example, HIPAA required Defendant to ensure the confidentiality of the electronic PHI it received and maintained by protecting against reasonably anticipated threats to its integrity. *Id*. § 160.306(a). To do so, Defendant was required to implement reasonable and appropriate security measures to mitigate the risk of unauthorized access to its patients' electronic personal health information, including by encrypting certain data where appropriate.[28]

49. Defendant failed to properly implement these basic data security practices. Defendant's failure to employ reasonable and appropriate measures to protect against unauthorized access to patients' Private Information constitutes an unfair act or practice prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45.

D. Plaintiff's Experiences

50. Plaintiff Leah Willis has been a patient of Ascension Providence Hospital –

[27] 45 C.F.R. § 160.103
[28] *See id.* §§ 164.308 (administrative safeguards), 164.312 (technical safeguards).

Southfield Campus in Southfield, Michigan since approximately 2018, and has obtained healthcare treatment from multiple Ascension Health physicians and healthcare providers since that time.

51. As a condition of obtaining medical services from Ascension Health, Plaintiff was required to provide her Personal Information to Defendant to be stored on their electronic network.

52. Upon information and belief, Defendant held Plaintiff's Personal Information on its electronic network at the time of the Data Breach.

53. As a result of learning of the Data Breach, Plaintiff spent time dealing with the consequences of the Data Breach, which includes, but is not limited to: checking and verifying credit agency reports; changing passwords on accounts; checking and verifying financial accounts for fraudulent activity.

54. Plaintiff suffered actual injury in the form of damages to and diminution of the value of Private Information—a form of intangible property that Plaintiff entrusted to Defendant for the purpose of medical care and treatment, which was compromised in and as a result of the Data Breach. In fact, since the Data Breach Plaintiff has seen an increase in spam and/or phishing emails and scam phone calls.

55. Plaintiff has also suffered lost time, annoyance, interference, and inconvenience as a result of the Data Breach. This is time Plaintiff otherwise would have spent performing other activities, such as work and/or leisurely activities for the enjoyment of life.

56. Plaintiff has also suffered costly and emotionally distressing delays in her healthcare because of the Data Breach and Defendant's failure to secure their network.

57. Prior to the Data Breach, Plaintiff was scheduled to undergo surgery and related healthcare at Ascension Health.

58. After the Data Breach, Plaintiff's doctors at Ascension Hospital needed to alter her

surgical plan, but could not do so, because Defendant's electronic health records system had shutdown, and were unable to proceed with Plaintiff's scheduled surgery.[29]

59. Due to the Data Breach and Defendant's resulting system shutdown, Plaintiff has had to search for a new doctor not associated with Ascension Health, which has caused her, and will cause her, additional harm and expenses in the form of months of delayed care, lost time and additional costs in transportation alone. Plaintiff's life has been in suspension as a result of the delay caused by Defendant's failure to secure their electronic system. The Data Breach and resulting delay in care has also caused Plaintiff additional emotional distress.

60. In sum, the Data Breach and the resulting disruptions in Plaintiff's healthcare, have impacted her both financially and emotionally.

61. Plaintiff has also suffered imminent and impending injury arising from the disclosure of her Private Information and for the substantially increased risk of fraud, identity theft, and misuse resulting from Private Information being placed in the hands of unauthorized third parties and criminals.

62. Plaintiff has a continued interest in ensuring that Private Information, which remains backed up and in Defendant's possession, is protected and safeguarded from further and future breaches.

E. Plaintiff and Class Members Suffered Damages

63. Defendant had a duty to keep Private Information confidential and to protect it from unauthorized access and disclosures. Plaintiff and Class Members provided their Private Information to Defendant with the understanding that Defendant and any business partners to whom Defendant disclosed Private Information would comply with their obligations to keep such

[29] *See* https://www.freep.com/story/news/health/2024/05/21/ascension-hospital-hack-ransomware-cyber-attack/73776557007/ (last visited June 7, 2024).

information confidential and secure from unauthorized disclosures.

64. The Data Breach creates a heightened security concern for patients of Defendant because their Private Information, including Social Security numbers, medical records and other sensitive financial and personal data was included.

65. Medical privacy is among the most important tenets of American healthcare. Patients must be able to trust their physicians, insurers, and pharmacies to protect their medical information from improper disclosure including, but not limited to, their health conditions and courses of treatment. Indeed, numerous state and federal laws require this.

66. The Federal Trade Commission ("FTC") defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority." 17 C.F.R. § 248.201. The FTC describes "identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person," including, among other things, "[n]ame, Social Security number, date of birth, official State or government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number." *Id.*

67. Theft of Social Security numbers creates a particularly alarming situation for victims because those numbers cannot easily be replaced. Indeed, the Social Security Administration stresses that the loss of an individual's Social Security number can lead to identity theft and extensive fraud:

> A dishonest person who has your Social Security number can use it to get other personal information about you. Identity thieves can use your number and your good credit to apply for more credit in your name. Then, they use the credit cards and don't pay the bills, it damages your credit. You may not find out that someone is using your number until you're turned down for credit, or you begin to get calls from unknown creditors demanding payment for items you never bought. Someone illegally using your Social Security number and assuming your identity can cause

a lot of problems.[30]

68. It is also difficult to obtain a new Social Security number. A breach victim would have to demonstrate ongoing harm from misuse of her Social Security number, and a new Social Security number will not be provided until after the harm has already been suffered by the victim.

69. Given the highly sensitive nature of Social Security numbers, theft of these numbers in combination with other personally identifying information may cause damage to victims for years.

70. The sensitive and permanent nature of medical records also leaves victims with little to no recourse. Data thieves can use medical records to sell them for a higher value than credit card information and can use that information to obtain loans or even expensive medical services in the victim's name.[31]

71. Defendant's data security obligations were particularly important given the substantial increases in data breaches in recent years – especially against healthcare networks – which are widely known to the public and to anyone in Defendant's industry.

72. Data breaches are not new. These types of attacks should be anticipated by companies that store sensitive and personally identifying information, and these companies must ensure that data privacy and security is adequate to protect against and prevent known attacks. Indeed, many health care companies have been subject to numerous data security incidents, such as Anthem, United Healthcare, and Premera Blue Cross.

73. It is well known among companies that store sensitive personally identifying information that sensitive information is valuable and frequently targeted by criminals.

---

[30] *See Identity Theft and Your Social Security Number*, Social Security Administration, https://www.ssa.gov/pubs/EN-05-10064.pdf (last visited June 7, 2024)..

[31] https://www.hipaajournal.com/why-do-criminals-target-medical-records/ (last visited June 7, 2024).

74. Identify theft victims are frequently required to spend many hours and large amounts of money repairing the impact to their credit. Identity thieves use stolen personal information for a variety of crimes, including credit card fraud, tax fraud, phone or utilities fraud, and bank/finance fraud.

75. There may be a time lag between when the harm occurs versus when it is discovered, and also between when Private Information is stolen and when it is used. According to the U.S. Government Accountability Office, which conducted a study regarding data breaches:

> [L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.[32]

76. Stolen health data in particular can go incredibly long periods without being detected. In that time, that data can be used to accrue large amounts of debt than is typically seen in other areas like credit cards and social security numbers which are more closely monitored.[33]

77. With access to an individual's Private Information, criminals can commit all manners of fraud, including obtaining a driver's license or official identification card in the victim's name but with the thief's picture, using the victim's name and Social Security number to obtain government benefits, or filing a fraudulent tax return using the victim's information.

78. Private Information is such a valuable commodity to identity thieves that once the information has been compromised, criminals often trade the information on the dark web and the "cyber black-market" for years. As a result of recent large-scale data breaches, identity thieves and cybercriminals have openly posted stolen Social Security numbers and other Private

---

[32] *See Report to Congressional Requesters*, U.S. Government Accountability Office, (June 2007), http://www.gao.gov/new.items/d07737.pdf. (last visited June 7, 2024).
[33] *See* https://www.hipaajournal.com/why-do-criminals-target-medical-records/ (last visited June 7, 2024).

Information directly on various illegal websites making the information publicly available, often for a price.

79. Moreover, a study found that the "average total cost" of medical identity theft is "about $20,000" per incident, and that a majority of victims of medical identity theft were forced to pay out-of-pocket costs for healthcare they did not receive in order to restore coverage.[34]

80. As an additional cost, stolen highly sensitive information from medical records such as "medical conditions, pregnancies, abortions, or sexual health tests" can be used by criminals for extortion or blackmail.[35]

81. Even if only some of Plaintiff's data was exposed in the Data Breach, partial records – especially medical records – can be sold to other cybercriminals on the dark web to create "fullz" packages, a full identity record set that is compiled from multiple cybercriminals and data breaches. "Fullz" packages allow cyber criminals extensive information that can be used further than that stolen in the original Data Breach.[36]

82. Any "fullz" package created using Plaintiff and Class Members' stolen data can be used and resold indefinitely, leading to extended harm.

83. Defendant is, and at all relevant times has been, aware that the Private Information it handles and stores in connection with providing healthcare services is highly sensitive. As a company that handles highly sensitive and identifying medical information, Defendant is aware of

[34] *See* Elinor Mills, *Study: Medical identity theft is costly for victims*, CNET, (Mar. 3, 2010, 5:00 a.m.), https://www.cnet.com/news/study-medical-identity-theft-is-costly-for-victims; see Annie Nova, *Here's how to avoid medical identity theft*, CNBC, (June 7, 2019 11:15 a.m.), https://www.cnbc.com/2019/06/07/how-to-avoid-medical-identity-theft.html. (last visited June 7, 2024).

[35] *See* https://www.hipaajournal.com/why-do-criminals-target-medical-records/ (last visited June 7, 2024).

[36] *See* https://www.hipaajournal.com/why-do-criminals-target-medical-records/ (last visited June 7, 2024).

the importance of safeguarding that information and protecting its systems and products from security vulnerabilities.

84. Despite the known risk of data breaches and the widespread publicity and industry alerts regarding other notable data breaches, Defendant failed to take reasonable steps to adequately protect its systems from being breached leaving its patients exposed to the risk of fraud and identity theft.

85. As a result of the events detailed herein, Plaintiff and Class Members suffered harm and loss of privacy, and will continue to suffer future harm, resulting from the Data Breach, including but not limited to: delayed medical care and treatment; costs associated with finding alternate healthcare providers and treatments; unnecessary pain and suffering, and emotional distress; invasion of privacy; loss of privacy; loss of control over personal information and identities; disclosure of their need for special education; disclosure of financial status; fraud and identity theft; unreimbursed losses relating to fraud and identity theft; loss of value and loss of possession and privacy of Private Information; harm resulting from damaged credit scores and information; loss of time and money preparing for and resolving fraud and identity theft; loss of time and money obtaining protections against future identity theft; and other harm resulting from the unauthorized use or threat of unauthorized exposure of Private Information.

86. As a result of the Data Breach, Plaintiff's and Class Members' privacy has been invaded, their Private Information is now in the hands of criminals, they face a substantially increased risk of identity theft and fraud, and they must take immediate and time-consuming action to protect themselves from such identity theft and fraud.

87. Had Defendant remedied the deficiencies in their data security systems and adopted security measures recommended by experts in the field, they would have prevented the intrusions

into its systems and, ultimately, the theft of Plaintiff's and Class Members' Private Information, and Defendant's provision of healthcare services would not have been interrupted.

88. As a direct and proximate result of Defendant's wrongful actions and inactions, Plaintiff and Class Members have been placed at an imminent, immediate, and continuing increased risk of harm from identity theft and fraud, requiring them to take the time which they otherwise would have dedicated to other life demands such as work and family in an effort to mitigate the actual and potential impact of the Data Breach on their lives.

89. The U.S. Department of Justice's Bureau of Justice Statistics found that "among victims who had personal information used for fraudulent purposes, twenty-nine percent spent a month or more resolving problems" and that "resolving the problems caused by identity theft [could] take more than a year for some victims."[37]

90. Defendant's failure to adequately protect Plaintiff's and Class Members' Private Information has resulted in Plaintiff and Class Members having to undertake these tasks, which require extensive amounts of time, calls, and, for many of the credit and fraud protection services, payment of money, and expending resources to locate other healthcare providers.

91. Plaintiff and Class Members have been damaged in several other ways as well. Plaintiff and Class Members have been exposed to an impending, imminent, and ongoing increased risk of fraud, identity theft, and other misuse of their Private Information. Plaintiff and Class Members must now and indefinitely closely monitor their financial and other accounts to guard against fraud. This is a burdensome and time-consuming activity. Class Members may have also purchased credit monitoring and other identity protection services, purchased credit reports, placed

[37] U.S. Department of Justice, Office of Justice Programs Bureau of Justice Statistics, *Victims of Identity Theft, 2012*, December 2013, *available at*: https://www.bjs.gov/content/pub/pdf/vit12.pdf (last visited June 7, 2024).

credit freezes and fraud alerts on their credit reports, and spent time investigating and disputing fraudulent or suspicious activity on their accounts. Plaintiff and Class Members also suffered a loss of the inherent value of their Private Information.

92. Plaintiff and Class members have also been damaged by being deprived of vital medical care, causing them to experience delayed treatment, costs associated with finding alternate healthcare providers and treatments; unnecessary pain and suffering, anxiety and emotional distress.

93. Private Information stolen in the Data Breach can be misused on its own, or it can be combined with personal information from other sources such as publicly available information, social media, etc., to create a package of information capable of being used to commit further identity theft. Thieves can also use the stolen Private Information to send spear-phishing emails to Class Members to trick them into revealing sensitive information. Lulled by a false sense of trust and familiarity from a seemingly valid sender (for example Wells Fargo, Amazon, or a government entity), the individual agrees to provide sensitive information requested in the email, such as login credentials, account numbers, and the like.

94. As a result of Defendant's failures to prevent the Data Breach, Plaintiff and Class Members have suffered, will suffer, and are at increased risk of suffering:

a. The compromise, publication, theft and/or unauthorized use of their Private Information;

b. Out-of-pocket costs associated with the prevention, detection, recovery and remediation from identity theft or fraud;

c. Lost opportunity costs and lost wages associated with efforts expended and the loss of productivity from addressing and attempting to mitigate the actual and future

consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest and recover from identity theft and fraud;

d. The continued risk to their Private Information, which remains in the possession of Defendant and is subject to further breaches so long as Defendant fails to undertake appropriate measures to protect the Private Information in their possession;

e. Current and future costs in terms of time, effort and money that will be expended to prevent, detect, contest, remediate and repair the impact of the Data Breach for the remainder of the lives of Plaintiff and Class Members;

f. Delay in obtaining and receiving healthcare from Ascension as a result of the Data Breach, which has resulted in, or may result in, physical, financial and/or emotional harm; and

g. Anxiety and distress resulting from fear of misuse of their Private Information, and/or the delay in obtaining medical services.

95. In addition to a remedy for the economic harm, Plaintiff and Class Members maintain an undeniable interest in ensuring that their Private Information is secure, remains secure, and is not subject to further misappropriation and theft.

CLASS ACTION ALLEGATIONS

96. Plaintiff brings this class action pursuant to Rule 23 of the Federal Rules of Civil Procedure on behalf of herself and on behalf of all others similarly situated.

97. The Nationwide Class that Plaintiff seeks to represent is defined as follows:

Nationwide Class:

All persons in the United States whose Private Information was exposed to unauthorized parties, or could not be accessed by Ascension, as a result of the data breach of Ascension Health that occurred in May 2024.

In addition to, or in the alternative to the Nationwide Class, Plaintiff seeks certification of the following state Sub-Class:

> **Michigan Sub-Class**:
>
> **All residents of Michigan whose Private Information was exposed to unauthorized third parties, or could not be accessed by Ascension, as a result of the data breach of Ascension Health that occurred in May 2024.**

98. Plaintiff reserves the right to modify, change, or expand the Class and Sub-Class definitions, including proposing additional subclasses, based on discovery and further investigation.

99. Excluded from the Classes are: (1) any Judge or Magistrate presiding over this action and members of their families; (2) Defendant, Defendant's subsidiaries, parents, successors, predecessors, and any entity in which Defendant has a controlling interest, and its current or former employees, officers, and directors; (3) counsel for Plaintiff and Defendant; and (4) legal representatives, successors, or assigns of any such excluded persons.

100. The Classes meet all of the criteria required by Federal Rule of Civil Procedure 23(a).

101. **Numerosity:** The Class Members are so numerous that joinder of all members is impracticable. Though the exact number and identities of Class Members are unknown at this time, it appears that the membership of the Classes are in the tens of thousands. The identities of Class members are also ascertainable through Defendant's records.

102. **Commonality:** Common questions of law and fact exist as to all Class Members. These common questions of law or fact predominate over any questions affecting only individual members of the Class. Common questions include, but are not limited to, the following:

a. Whether and to what extent Defendant had a duty to protect the Private

Information of Plaintiff and Class Members;

b. Whether Defendant failed to adequately safeguard the Private Information of Plaintiff and Class Members;

c. Whether Defendant adequately, promptly, and accurately informed Plaintiff and Class Members that their Private Information had been compromised;

d. Whether Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;

e. Whether Defendant adequately addressed and fixed the vulnerabilities which permitted the Data Breach to occur;

f. Whether Defendant was negligent or negligent *per se*;

g. Whether Plaintiff and Class Members are entitled to relief from Defendant as a result of Defendant's misconduct, and if so, in what amounts; and

h. Whether Class Members are entitled to injunctive and/or declaratory relief to address the imminent and ongoing harm faced as a result of the Data Breach.

103. **Typicality:** Plaintiff's claims are typical of the claims of the Classes she seeks to represent, in that the named Plaintiff and all members of the proposed Classes have suffered similar injuries as a result of the same misconduct alleged herein. Plaintiff has no interests adverse to the interests of the other members of the Classes.

104. **Adequacy:** Plaintiff will fairly and adequately protect the interests of the Classes and has retained attorneys well experienced in class actions and complex litigation as counsel, including cases alleging breach of privacy and negligence claims arising from corporate misconduct.

105. The Classes also satisfy the criteria for certification under Federal Rule of Civil Procedure 23(b) and 23(c). Among other things, Plaintiff avers that the prosecution of separate actions by the individual members of the proposed class would create a risk of inconsistent or varying adjudication which would establish incompatible standards of conduct for Defendant; that the prosecution of separate actions by individual class members would create a risk of adjudications with respect to them which would, as a practical matter, be dispositive of the interests of other Class Members not parties to the adjudications, or substantially impair or impede their ability to protect their interests; that Defendant has acted or refused to act on grounds that apply generally to the proposed Classes, thereby making final injunctive relief or declaratory relief described herein appropriate with respect to the proposed Classes as a whole; that questions of law or fact common to the Classes predominate over any questions affecting only individual members and that class action treatment is superior to other available methods for the fair and efficient adjudication of the controversy which is the subject of this action. Plaintiff also avers that certification of one or more subclasses or issues may be appropriate for certification under Federal Rule of Civil Procedure 23(c). Plaintiff further states that the interests of judicial economy will be served by concentrating litigation concerning these claims in this Court, and that the management of the Classes will not be difficult.

106. Plaintiff and other members of the Classes have suffered damages as a result of Defendant's unlawful and wrongful conduct. Absent a class action, Defendant's unlawful and improper conduct shall, in large measure, not go remedied. Absent a class action, the members of the Classes will not be able to effectively litigate these claims and will suffer further losses.

CLAIMS FOR RELIEF

COUNT I
Negligence

107. Plaintiff realleges each and every allegation contained above and incorporates by reference all other paragraphs of this Complaint as if fully set forth herein.

108. Plaintiff brings this claim on behalf of the Class, or in the alternative, the Michigan Sub-Class.

109. Defendant negligently represented that it would safeguard Private Information despite leaving Plaintiff's and the Classes' Private Information exposed to unauthorized access.

110. Defendant was entrusted with, stored, and otherwise had access to the Private Information of Plaintiff and Class Members.[38]

111. Defendant knew, or should have known, of the risks inherent to storing the Private Information of Plaintiff and Class Members, and to not ensuring that its products and services were secure. These risks were reasonably foreseeable to Defendant.

112. Defendant owed duties of care to Plaintiff and Class Members whose Private Information had been entrusted to them.

113. Further, after discovering that cybercriminals had infiltrated its systems, Defendant failed to timely notify patients, consequently, causing notice to Plaintiff and Class Members to be untimely and insufficient to identify what Private Information had been exposed.

114. Defendant had additional duties to safeguard Plaintiff's and Class Members' data through the following statutes and regulations:

a. Pursuant to the FTC Act, 15 U.S.C. § 45, Defendant had a duty to provide

[38] As used herein, "Plaintiff and Class Members" includes members of the proposed Class and the Sub-Class.

fair and adequate computer systems and data security practices to safeguard Plaintiff's and Class Members' Private Information.

b. Pursuant to HIPAA, 42 U.S.C. § 1320d, Defendant had a duty to securely store and maintain the Plaintiff's and Class Members' PHI.

115. Defendant's duty to use reasonable care in protecting confidential data arose not only as a result of the statutes and regulations described above, but also because Defendant is bound by industry standards to protect confidential Private Information.

116. Defendant breached its duties, and thus was negligent, by failing to use reasonable measures to protect the Plaintiff's and Class Members' Private Information. The specific negligent acts and omissions committed by Defendant include, but are not limited to, the following:

a. Failing to adopt, implement, and maintain adequate security measures to safeguard Plaintiff's and Class Members' Private Information;

b. Failing to adequately monitor the security of its networks and systems;

c. Allowing unauthorized access to and exfiltration of Plaintiff's and Class Members' Private Information;

d. Failing to timely detect that Plaintiff's and Class Members' Private Information had been compromised;

e. Failing to ensure that it could access and maintain Class Members' Private Information and thus continue to provide treatment to them;

f. Failing to provide timely notice that Plaintiff's and Class Members' Private Information had been compromised so those at risk could take timely and appropriate steps to mitigate the potential for identity theft and other damages; and

g. Failing to provide adequate notice of what Private Information had been

compromised so that Plaintiff and Class Members at risk could take timely and appropriate steps to mitigate the potential for identify theft and other damages.

117. It was foreseeable to Defendant that its failure to use reasonable measures to protect Plaintiff's and Class Members' Private Information would result in injury to Plaintiff and Class and Sub-Class members. Further, the breach of security was reasonably foreseeable given the known high frequency of ransomware attacks and data breaches.

118. It was additionally foreseeable to Defendant that failure to timely and adequately provide notice of the Data Breach would result in Plaintiff and Class Members not being afforded the ability to timely safeguard their identities.

119. Defendant breached its duties to Plaintiff and Class Members by failing to provide fair, reasonable, or adequate data security in connection to its services. Defendant had a duty to safeguard Plaintiff's and Class Members' Private Information and to ensure that their systems and products adequately protected the Private Information.

120. But for Defendant's wrongful and negligent breach of its duties owed to Plaintiff and Class Members, Plaintiff and Class Members would not have been injured.

121. Defendant acted with wanton disregard for the security of Plaintiff's and Class Members' Private Information.

122. The injury and harm suffered by Plaintiff and Class Members was the reasonably foreseeable result of Defendant's breach of its duties. Defendant knew or should have known that it was failing to meet its duties, and that Defendant's breach would cause Plaintiff and Class Members to experience the foreseeable harms associated with the exposure of their Private Information.

123. As a direct and proximate result of Defendant's negligent conduct, Plaintiff and

Class Members have suffered injury, including but not limited to: (i) actual identity theft; (ii) the loss of the opportunity of how their Private Information is used; (iii) the compromise, publication, and/or theft of their Private Information; (iv) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their Private Information; (v) the continued risk to their Private Information, which may remain in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect Plaintiff's and Class Members' Private Information in its continued possession; (vi) delayed medical care and treatment, costs associated with finding alternate healthcare providers and treatments, and unnecessary pain and suffering, and emotional distress; and (vii) future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the Private Information compromised as a result of the Data Breach for the remainder of the lives of Plaintiff and Class Members.

124. As a direct and proximate result of Defendant's negligent conduct, Plaintiff and Class Members face an increased risk of future harm.

125. Plaintiff is entitled to compensatory and consequential damages suffered as a result of the Data Breach.

126. Plaintiff is also entitled to injunctive relief requiring Defendant to, e.g., (i) strengthen its data security programs and monitoring procedures; (ii) submit to future annual audits of those systems and monitoring procedures; and (iii) immediately provide robust and adequate credit monitoring to all Class members, and any other relief this Court deems just and proper.

127. As a direct and proximate result of Defendant's negligent conduct, Plaintiff and Class Members and are entitled to damages in an amount to be proven at trial.

COUNT II
Negligence Per Se

128. Plaintiff realleges each and every allegation contained above and incorporates by reference all other paragraphs of this Complaint as if fully set forth herein.

129. Plaintiff brings this claim on behalf of the Class, or in the alternative, the Michigan Sub-Class.

130. Pursuant to the Federal Trade Commission Act ("FTC Act"), 15 U.S.C. § 45, Defendant had a duty to provide adequate data security practices to safeguard Plaintiff's and Class Members' Private Information.

131. Pursuant to HIPAA, 42 U.S.C. § 1320d, Defendant had a duty to securely store and maintain the Plaintiff's and Class Members' PHI.

132. Pursuant to other state and federal laws requiring the confidentiality of Private Information, including, but not limited to, the FTC Act and HIPAA, among other laws, Defendant had a duty to implement reasonably safeguards to protect Plaintiff's and Class Members' Private Information.

133. Defendant breached its duties to Plaintiff and Class Members under the FTC Act and HIPAA, among other laws, by failing to provide fair, reasonable, or adequate data security in order to safeguard Plaintiff's and Class Members' Private Information.

134. Defendant's failure to comply with applicable laws and regulations constitutes negligence per se.

135. But for Defendant's wrongful and negligent breach of its duties owed to Plaintiff and Class Members, Plaintiff and Class Members would not have been injured.

136. The injury and harm suffered by Plaintiff and Class Members was the reasonably foreseeable result of Defendant's breach of its duties. Defendant knew or should have known that

it was failing to meet its duties, and that its breach would cause Plaintiff and Class Members to experience the foreseeable harms associated with the exposure of their Private Information and .

137. As a direct and proximate result of Defendant's negligent conduct, Plaintiff and Class Members face an increased risk of future harm.

138. As a direct and proximate result of Defendant's negligent conduct, Plaintiff and Class Members have suffered injury and are entitled to damages in an amount to be proven at trial.

COUNT III
Breach of Express and/or Implied Contract

139. Plaintiff realleges each and every allegation contained above and incorporates by reference all other paragraphs of this Complaint as if fully set forth herein.

140. Plaintiff brings this claim on behalf of the Class, or in the alternative, the Michigan Sub-Class.

141. Plaintiff and Class Members provided their Private Information to Defendant with the explicit and implicit understandings that Defendant would take precautions to protect that Private Information from unauthorized disclosure.

142. Plaintiff and Class Members are parties to contracts with Defendant. Under the circumstances, recognition of a right to performance by Plaintiff and Class Members is appropriate to effectuate the intentions of the parties to these contracts. One or more of the parties to these contracts intended to give Plaintiff and Class Members the benefit of the performance promised in the contracts.

143. Defendant breached these express and/or implied agreements, which directly and/or proximately caused Plaintiff and Class Members to suffer substantial damages.

144. Accordingly, Plaintiff and Class Members are entitled to damages, restitution, disgorgement of profits and other relief in an amount to be proven at trial.

COUNT IV
Invasion of Privacy

145. Plaintiff realleges each and every allegation contained above and incorporates by reference all other paragraphs of this Complaint as if fully set forth herein.

146. Plaintiff brings this claim on behalf of the Class, or in the alternative, the Michigan Sub-Class.

147. Plaintiff and Class Members had a legitimate and reasonable expectation of privacy with respect to their Private Information and were accordingly entitled to the protection of this information against disclosure to unauthorized third parties.

148. Defendant owed a duty to its patients, including Plaintiff and Class Members, to keep their Private Information confidential.

149. The unauthorized release of Private Information, especially the type related to medical information, is highly offensive to a reasonable person.

150. The intrusion was into a place or thing, which was private and is entitled to be private. Plaintiff and Class Members disclosed their Private Information to Defendant as part of their use of Defendant's services, but privately, with the intention that the Private Information would be kept confidential and protected from unauthorized disclosure. Plaintiff and Class Members were reasonable in their belief that such information would be kept private and would not be disclosed without their authorization.

151. The Data Breach constitutes an intentional interference with Plaintiff's and Class Members' interest in solitude or seclusion, either as to their persons or as to their private affairs or concerns, of a kind that would be highly offensive to a reasonable person.

152. Defendant acted with a knowing state of mind when they permitted the Data Breach because it knew its information security practices were inadequate and would likely result in a data

breach such as the one that harmed Plaintiff and Class Members.

153. Acting with knowledge, Defendant had notice and knew that its inadequate cybersecurity practices would cause injury to Plaintiff and Class Members.

154. As a proximate result of Defendant's acts and omissions, Plaintiff's and Class Members' Private Information was disclosed to and used by third parties without authorization in the manner described above, causing Plaintiff and Class Members to suffer damages.

155. Unless and until enjoined, and restrained by order of this Court, Defendant's wrongful conduct will continue to cause great and irreparable injury to Plaintiff and Class Members in that the Private Information maintained by Defendant can be viewed, distributed, and used by unauthorized persons.

156. Plaintiff and Class Members have no adequate remedy at law for the injuries in that a judgment for monetary damages will not end the invasion of privacy for Plaintiff and Class Members.

COUNT V
Michigan Identity Theft Protection Act,
Mich. Comp. Laws Ann. § 445.72, *et seq.*

157. Plaintiff realleges each and every allegation contained above and incorporate by reference all other paragraphs of this Complaint as if fully set forth herein.

158. Plaintiff brings this claim on behalf of herself and the Michigan Sub-Class.

159. Defendant is a business that owns or licenses computerized data that includes "Personal Information" (for the purpose of this count, "Private Information") within the meaning of Mich. Comp. Laws Ann. § 445.72(1).

160. Plaintiff and Sub-Class Members' PII and PHI includes Personal Information as defined by Mich. Comp. Laws Ann. § 445.72(1).

161. Defendant is required to accurately notify Plaintiff and Sub-Class Members if it

discovers a security breach, or receives notice of a security breach (where unencrypted and unredacted Private Information was accessed or acquired by unauthorized persons), without unreasonable delay under Mich. Comp. Laws Ann. § 445.72(1).

162. Defendant was required to provide written notice in a "clear and conspicuous manner." Mich. Comp. Laws Ann. § 445.72(6).

163. Because Defendant discovered a security breach and had notice of a security breach (where Private Information was accessed or acquired by unauthorized persons), Defendant had an obligation to disclose the Data Breach in a timely and accurate fashion as mandated by Mich. Comp. Laws Ann. § 445.72(4).

164. By failing to disclose the Data Breach in a timely and accurate manner and provide clear and conspicuous notice, Defendant violated Mich. Comp. Laws Ann. § 445.72(4).

165. As a direct and proximate result of Defendant's violations of Mich. Comp. Laws Ann. § 445.72(4), Plaintiff and Sub-Class Members suffered damages, and will continue to suffer damages, as described above.

166. Plaintiff and Sub-Class Members seek relief under Mich. Comp. Laws Ann. § 445.72(13), including a civil fine.

COUNT VI
Michigan Consumer Protection Act,
Mich. Comp. Laws Ann. § 445.903, *et seq*.

167. Plaintiff realleges each and every allegation contained above and incorporates by reference all other paragraphs of this Complaint as if fully set forth herein.

168. Plaintiff brings this claim on behalf of the Michigan Sub-Class.

169. Defendant and Michigan Sub-Class are "persons" under Mich. Comp. Laws Ann. § 445.902(d).

170. Defendant advertised, offered, or sold goods or services in Michigan and engaged

in trade or commerce directly or indirectly affecting the people of Michigan, as defined by Mich. Comp. Laws Ann. § 445.903(g).

171. Defendant engaged in unfair and deceptive acts and practices in or affecting commerce, in violation of Mich. Comp. Laws Ann. § 445.903(1), including:

a. Representing their goods and services to have characteristics, uses and benefits which they did not have, violating Mich. Comp. Laws Ann. § 445.903(1)(c).

b. Making a representation material to Plaintiff and Sub-Class's transaction such that one reasonably believes the represented state of Defendant's affairs to be something which it is not, in violation of Mich. Comp. Laws Ann. § 445.903(1)(bb).

c. Failing to reveal facts material to Plaintiff and Sub-Class's transaction in light of representations of fact made in a positive manner, in violation of Mich. Comp. Laws Ann. § 445.903(1)(cc).

d. Failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, and adequately improve security and privacy measures following previous cybersecurity incidents, which was a direct and proximate cause of the Data Breach;

e. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff and Sub-Class Members' Private Information, which was a direct and proximate cause of the Data Breach;

f. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Sub-Class Members' Private

Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, HIPAA, and other laws, which was a direct and proximate cause of the Data Breach;

g. Failing to ensure that it could access and maintain Class Members' Private Information on its systems and thus continue to provide treatment to them;

h. Misrepresenting that they would protect the privacy and confidentiality of Plaintiff's and Sub-Class Members' Private Information, including by implementing and maintaining reasonable security measures;

i. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and Sub-Class Members' PII, including duties imposed by the and the FTC Act, 15 U.S.C. § 45, HIPAA, and other laws;

j. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff and Sub-Class Members' Private Information;

k. Failing to timely notify Plaintiff and Sub-Class Members of the Data Breach violation under the Michigan Identity Theft Protection Act, Mich. Comp. Laws Ann. § 445.72(1).

172. Defendant's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Defendant's data security and ability to protect the confidentiality of consumers' Private Information.

173. Defendant intended to mislead Plaintiff and Sub-Class Members and induce them to rely on its misrepresentations and omissions.

174. Had Defendant disclosed to Plaintiff and Class Members that its systems were not secure and, thus, vulnerable to attack, Defendant would have been unable to continue in business and it would have been forced to adopt reasonable data security measures and comply with the law. Instead, Defendant was trusted with sensitive and valuable Private Information regarding hundreds of thousands of consumers, including Plaintiff, Class Members, and Sub-Class Members. Defendant accepted the responsibility of being a steward of this data while keeping the inadequate state of its security controls secret from the public. Accordingly, because Defendant held itself out as maintaining a secure platform for Private Information data, Plaintiff, Class Members, and Sub-Class Members acted reasonably in relying on Defendant's misrepresentations and omissions, the truth of which they could not have discovered.

175. Defendant acted intentionally, knowingly, and maliciously to violate Michigan's Consumer Protection Act, and recklessly disregarded Plaintiff and Sub-Class Members' rights.

176. As a direct and proximate result of Defendant's unfair and deceptive acts and practices, Plaintiff and Sub-Class Members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including from fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; loss of value of their Private Information; and delayed medical care and treatment, costs associated with finding alternate healthcare providers and treatments, and unnecessary pain and suffering, and emotional distress.

177. Plaintiff and Sub-Class Members seek all monetary and non-monetary relief allowed by law, including the greater of actual damages, restitution, injunctive relief, and any other relief that is just and proper.

COUNT VII
Declaratory Judgement

178. Plaintiff realleges each and every allegation above and incorporates by reference all other paragraphs of this Complaint as if fully set forth herein.

179. Plaintiff brings this claim on behalf of the Class, or in the alternative, the Michigan Sub-Class.

180. Plaintiff and the Class have stated claims against Defendant for common law torts and statutory violations.

181. Defendant failed to fulfill its obligations to provide adequate and reasonable data security measures for the Private Information of Plaintiff and the Class, as evidenced by the Data Breach.

182. As a result of the Data Breach, Defendant's systems are more vulnerable to access by unauthorized parties and require more stringent measures to be taken to safeguard the Plaintiff's and Class Members' Personal Information going forward.

183. As a result of the Data Breach, Defendant's systems were unable to provide healthcare services to Class Members whose data it could not access on its systems;

184. An actual controversy has arisen in the wake of the Data Breach regarding Defendant's current obligations to provide data security measures that will adequately protect Plaintiff's and Class Members' Private Information.

185. Plaintiff seeks a declaration that Defendant must implement specific additional, prudent, industry-standard data security practices to provide reasonable protection and security to Plaintiff and Class Members' Private Information and to ensure that it not again impeded in the provision of healthcare services. Specifically, Plaintiff and the Class seek a declaration that Defendant's existing security measures do not comply with its obligations, and that Defendant

must implement and maintain reasonable data security measures on behalf of Plaintiff and the Class to comply with its data security obligations.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, on behalf of herself and on behalf of the Classes, pray for relief as follows:

A. For an Order certifying this case as a class action pursuant to Federal Rule of Civil Procedure 23 against Defendant, appointing Plaintiff as Class Representative of the Class and/or Sub-Classes;

B. Awarding monetary, punitive and actual damages and/or restitution, as appropriate;

C. Awarding declaratory and injunctive relief as permitted by law or equity to assure that the Classes have an effective remedy, including enjoining Defendant from continuing the unlawful practices as set forth above;

D. Prejudgment interest to the extent allowed by the law;

E. Awarding all costs, experts' fees and attorneys' fees, expenses and costs of prosecuting this action; and

F. Such other and further relief as the Court may deem just and proper.

JURY TRIAL DEMAND

Plaintiff demands a trial by jury on all issues so triable.

DATED: June 13, 2024

Respectfully submitted,

STUEVE SIEGEL HANSON LLP

/s/ Norman E. Siegel
Norman E. Siegel – 44378MO
J. Austin Moore – 64040MO
460 Nichols Road, Suite 200
Kansas City, Missouri 64112
T: 816-714-7100
siegel@stuevesiegel.com
moore@stuevesiegel.com

KAPLAN FOX & KILSHEIMER LLP
Laurence D. King, Esq. (*pro hac vice* application forthcoming)
Matthew B. George, Esq. (*pro hac vice* application forthcoming)
Blair E. Reed, Esq. (*pro hac vice* application forthcoming)
Clarissa R. Olivares, Esq. (*pro hac vice* application forthcoming)
1999 Harrison Street, Suite 1560
Oakland, CA 94612
T: 415-772-4700
F: 415-772-4707
lking@kaplanfox.com
mgeorge@kaplanfox.com
breed@kaplanfox.com
colivares@kaplanfox.com

KAPLAN FOX & KILSHEIMER LLP
Peter S. Linden, Esq. (*pro hac vice* application forthcoming)
800 Third Avenue, 38th Floor
New York, NY 10022
T: 212-687-1980
F: 212-687-7714
plinden@kaplanfox.com

Attorneys for Plaintiff and the Proposed Class